CLAIMS

What is claimed is:

1. A method for synchronizing a ciphering key change in a wireless communications system, the wireless communications system comprising:

a first station capable of receiving a security mode command to effect a ciphering change, and capable of receiving encrypted layer 2 protocol data units (PDUs), each received PDU being sequentially identified by an n-bit frame number (FN), the first station comprising:

a first m-bit hyper frame number (HFN); and

a decryption unit capable of decrypting received PDUs according to at least a first ciphering key, the first HFN, and the FN of each received PDU; and

a second station capable of transmitting the security mode command, and capable of transmitting encrypted PDUs, the second station comprising:

a second m-bit HFN; and

an encryption unit capable of encrypting transmitted PDUs according to at least the first ciphering key, the second HFN, and an FN associated with each transmitted PDU;

the method comprising:

the second station determining an activation time at which a ciphering key change is to occur;

the second station composing the security mode command, the security mode command comprising a switching FN corresponding to the activation time, and x least-significant bits (LSBs) from the second HFN corresponding to the activation time;

the second station transmitting the security mode command;

the first station receiving the security mode command;

the first station utilizing the switching FN and the x LSBs from the second HFN contained in the security mode command to obtain an application time; and

the first station using the first ciphering key to decrypt PDUs with FNs sequentially prior to the application time, and using a second ciphering key to decrypt PDUs with FNs sequentially on or after the application time.

2. The method of claim 1 wherein the first station increments the first HFN by a predetermined value on detection of roll-over of an FN of a received PDU.

3. The method of claim 1 wherein the second station increments the second HFN by a predetermined value on detection of roll-over of an FN of a transmitted PDU.

4. The method of claim 1 wherein the first HFN and the second HFN are synchronized.

5. The method of claim 4 wherein the activation time corresponds to a second HFN/FN sequence pair for a crossover PDU, the crossover PDU being the sequentially earliest PDU encrypted using the second ciphering key, and the application time corresponds to a synchronized first HFN/FN sequence pair for a corresponding received PDU.

6. The method of claim 5 wherein the switching FN is the FN of the crossover PDU, and the x LSBs are extracted from the second HFN corresponding to the crossover PDU.

7. The method of claim 1 wherein the activation time is equal to the application time.

8. The method of claim 1 wherein x is greater than or equal to 2.

9. The method of claim 1 wherein x is equal to m.

10. The method of claim 1 wherein the first station compares the x LSBs from the second HFN contained in the security mode command to determine a cyclical positioning of the switching FN within the first HFN.

11. A wireless communications system comprising:

a first station capable of receiving encrypted layer 2 protocol data units (PDUs), and capable of receiving a security mode command, the first station comprising:

a receiving buffer for storing received PDUs, the first station associating a sequentially ordered n-bit frame number (FN) and an m-bit hyper frame number (HFN) with each received PDU;

an extraction unit for obtaining an application time from a switching FN and x least significant bits (LSBs) of a second HFN, the switching FN and the x LSBs of the second HFN contained in the security mode command;

a first ciphering key;

a second ciphering key; and

a decryption unit for decrypting the received PDUs, the decryption unit using the first ciphering key to decrypt any received PDU with an HFN/FN pair that is sequentially before the application time,

and using the second ciphering key to decrypt any received PDU with an HFN/FN pair that is sequentially on or after the application time.

12. The system of claim 11 further comprising a second station capable of transmitting the security mode command, and capable of transmitting the encrypted PDUs; wherein PDUs that are sequentially before the application time are encrypted using the first ciphering key, and PDUs sequentially on or after the application time are encrypted using the second ciphering key.

13. The system of claim 12 wherein the HFN of each received PDU is synchronized with a corresponding HFN on the second station for each PDU transmitted by the second station.

14. The system of claim 13 wherein the second station comprises an encryption unit capable of generating an activation time, the activation time corresponding to an HFN/FN sequence pair for a crossover PDU, the crossover PDU being the sequentially earliest PDU encrypted by the encryption unit using the second ciphering key, and the application time corresponds to a synchronized HFN/FN sequence pair for a corresponding PDU received by the first station.

15. The system of claim 14 wherein the switching FN is the FN of the crossover PDU, and the second HFN is the HFN of the crossover PDU.

16. The system of claim 14 wherein the activation time is equal to the application time.

17. The system of claim 11 wherein the first station increments the HFN associated with a first PDU by a predetermined value on rollover of the FN associated with the first PDU.

18. The system of claim 11 wherein x is greater than or equal to 2.

19. The system of claim 11 wherein x is equal to m.

20. A data structure for use in a wireless communications system to synchronize a ciphering key change in the wireless communications system, the wireless communications system comprising:

a first station capable of receiving encrypted layer 2 protocol data units (PDUs), assigning a first n-bit frame number (FN) and a first m-bit hyper frame number (HFN) to each received PDU to generate a first HFN/FN pair for each received PDU, and decrypting each received PDU according to the first HFN/FN pair, an application time, a first ciphering key, and a second ciphering key, the first station using the first ciphering key if the first HFN/FN pair is sequentially before the application time, and using the second ciphering key if the first HFN/FN pair is sequentially on or after the application time; and

a second station capable of transmitting the encrypted PDUs, the second station assigning a second n-bit FN and a second m-bit HFN to each PDU to be transmitted to generate a second HFN/FN pair for each PDU to be transmitted, and encrypting each PDU to be transmitted according to the second HFN/FN pair, an activation time, a third ciphering key, and a fourth ciphering key, the

second station using the third ciphering key if the second HFN/FN pair is sequentially before the activation time, and using the fourth ciphering key if the second HFN/FN pair is sequentially on or after the activation time;

the data structure comprising:

x least significant bits (LSBs) of a second HFN corresponding to the activation time; and

a switching FN corresponding to the activation time;

wherein the second station composes the data structure and transmits the data structure to the first station to enable the first station to synchronize the application time with the activation time.

21. The data structure of claim 20 wherein the switching FN is the FN of a second HFN/FN pair of a crossover PDU transmitted by the second station, the crossover PDU being the sequentially earliest PDU encrypted using the fourth ciphering key, and the x LSBs are extracted from the HFN of the second HFN/FN pair of the crossover PDU.

22. The data structure of claim 20 wherein x is two.

23. The data structure of claim 20 wherein the third ciphering key is associated with the first ciphering key, and the fourth ciphering key is associated with the second ciphering key.

24. The data structure of claim 23 wherein the third ciphering key is identical to the first ciphering key, and the fourth ciphering key is identical to the second ciphering key.

25. A method for removing cyclical ambiguity of an n-bit

identifying frame number (FN) transmitted in a signaling message from a first station to a second station in a wireless communications system, the identifying FN identifying a layer 2 protocol data unit (PDU) in a stream of PDUs, the first station comprising a first m-bit hyper frame number (HFN) that is incremented by a first value upon detection of roll-over of an FN in the stream of PDUs, each PDU in the stream of PDUs having an associated FN value and each FN value having an associated HFN value, the method comprising:

the first station placing the identifying FN into a first field of a message;

the first station placing x least significant bits (LSBs) from the HFN value associated with the identifying FN in a second field of the message; and

the first station transmitting the message to the second station;

wherein after reception of the message, the second station uses the x LSBs of the second field to determine a cyclical position of the identifying FN.

26. The method of claim 25 wherein x is greater than or equal to two.

27. The method of claim 25 wherein the second station has a second HFN that is synchronized with the HFN of the first station, and the second station uses the x LSBs of the second field to determine the cyclical position of the identifying FN within the second HFN.